State of Washington
Decision Package

Agency: **310 Department of Corrections**
Decision Package Code/Title: **0E – Regulatory Compliance**

Budget Period: **2005-07**

Budget Level: **M2 – Inflation and Other Rate Changes**

Recommendation Summary Text:
The Department requests funds required for regulatory compliance.

Agency Total

Fiscal Detail	**FY 2006**	**FY 2007**	**Total**
Operating Expenditures			
001-1 - General Fund – Basic Account-State	$2,359,000	$1,124,000	$3,483,000

Staffing	**FY 2006**	**FY 2007**	**Annual Average**
FTEs	12.0	12.0	12.0

Program 100-Admin & Program Support

Fiscal Detail	**FY 2006**	**FY 2007**	**Total**
Operating Expenditures			
001-1 - General Fund – Basic Account-State	$1,704,000	$889,000	$2,593,000

Staffing	**FY 2006**	**FY 2007**	**Annual Average**
FTEs	9.0	9.0	9.0

Program 200-Institutional Services

Fiscal Detail	**FY 2006**	**FY 2007**	**Total**
Operating Expenditures			
001-1 - General Fund – Basic Account-State	$352,000	$58,000	$410,000

Staffing	**FY 2006**	**FY 2007**	**Annual Average**
FTEs	N/A	N/A	N/A

Program 300-Community Corrections

Fiscal Detail	FY 2006	FY 2007	Total
Operating Expenditures			
001-1 - General Fund – Basic Account-State	$303,000	$177,000	$480,000

Staffing	FY 2006	FY 2007	Annual Average
FTEs	3.0	3.0	3.0

Package Description

The Department requests funding to meet recent changes in applicable regulatory requirements. These changes have been imposed on the Department by other state agencies and local municipalities.

Fire Inspection

A recent fire inspection at Larch Corrections Center (LCC) that occurred on March 18, 2004 determined that LCC must immediately comply with the requirement of testing the fire alarm system on an annual basis. The National Fire Protection Association (NFPA) requires that the fire alarm system be tested for reliability every year and sensitivity testing every other year. LCC has not performed this function in the past. Funding is requested in the amount of $34,000 to have these tests performed on an annual basis.

Interstate Compact Requirements

Three additional positions are required to handle the increased workload resulting from recent rules passed by the Interstate Compact Commission. The Interstate Compact Commission has the statutory authority for regulating the transfer of adult offenders under state supervision across state boundaries. In November 2003, the Commission adopted new rules, which have an implementation date of August 2004. The rules have significant changes that affect the way in which the Department does business. The new rules require more accountability of the offender, state and national level oversight, and an enforcement mechanism. Also under new rules, Washington State is required to process the transfer of certain crime category misdemeanor offenders coming to or leaving our state through the Interstate Compact Office. Currently, misdemeanor offenders sentenced in our state are under either municipal or county jurisdiction and have not been transferred under this process. For misdemeanor offenders from other states requesting transfer through their Interstate Compact Office that meet the criteria for acceptance, Washington State must approve transfer. The obligation of supervision of these misdemeanor cases would seem to fall under the municipal or county jurisdiction in which the offender will reside. These jurisdictions have the ability to supervise these cases similar to the way they supervise their Washington State cases. A determination will need to be made if legislation is needed to provide the structure, the accountability, and the responsibility for non-compliance since the rules to implement this compact and our legislation further defines the requirements that was not known at the time our state implemented the legislation to become a party to the new compact. Until this issue is resolved, the Department is not requesting any additional resources for the increased workload that may result from the changes in regard to the misdemeanant offenders.

Exchange Upgrade

The Department must upgrade to Exchange 2003 and upgrade its enterprise computer network for 250 servers to the Windows 2003 operating system in order to maintain its presence in the "Washington State Forest." The Department request funding for the following to successfully implement the upgrades:

- Upgrade the current Microsoft Exchange Server 5.5 Software System to the new version of Exchange Server 2003. The Exchange Server System is Microsoft's messaging and collaboration server software that runs on the Department's servers and enables us to send and receive electronic mail. It

is designed to inter-operate with a software client application such as Microsoft Outlook. Exchange Server 2003 must run on servers running Microsoft Windows Server 2003 operating system.
- Upgrade all Department server operating systems to Windows 2003 Server System. Windows Server 2003 is an infrastructure platform for connecting applications, networks, and Web servers together.
- Additional funding to add 12 new domain controller servers to the Department's networks for the implementation of "Active Directory." Active Directory is a system that provides the means to manage the identities and relationships that make up the network environments. Windows Server 2003 makes Active Directory simpler to manage, easing migration, and deployment. All other servers have been upgraded to Windows 2003 or will be replaced and upgraded when purchased.
- Include funding for two additional network staff, ongoing training dollars for the entire network team, Microsoft's System Management Services software tools, and technical consulting services. One position will become the system administrator of the management tools and the new operational framework for Active Directory environments. The second position will manage the system architecture, structures, and monitor the secure system configuration.

The Department considers email to be a mission critical information technology service. Staff, contractors, even volunteers rely on this service in many ways. It provides a vital, efficient communication link between the geographically dispersed facilities and offices of the Department. Business processes such as the recently implemented Offender Accountability Plan, even our purchasing process depend on email. Therefore, it is of the highest priority for the Department to maintain the integrity, vitality, and security of its Microsoft Exchange platform on which this service is delivered.

Exchange 2003:
The Department must upgrade from Microsoft Exchange Server 5.5 to Exchange Server 2003. This is because Microsoft no longer supports its older mail services Exchange Server 5.5 system. The Department is vulnerable to system failure that would affect mission critical email services. The Department of Information Services (DIS) plans to move the entire "Washington State Forest" forward to Exchange Server 2003 during the next 12 months. Once DIS implements Exchange 2003, the Department will no longer be able to connect to the DIS State Exchange HUB unless the upgrade is completed. The Department requests funding for Exchange 2003 related software and ongoing support.

Windows 2003:
In order to upgrade to Exchange 2003, the Department must also implement the Windows 2003 Server operating system across the Department's network. Additional funding to add 12 new servers to the network as domain controllers is needed based on recommendations from Microsoft and DIS regarding implementation of "Active Directory." All other servers have been upgraded to Windows 2003 or will be replaced with new servers that include the Windows 2003 Server operating system when purchased through the biennial replacement cycle.

Network Operational Framework:
Because the Department's enterprise network and email services are mission critical systems that support all staff and computer applications, this upgrade must be conducted in accordance with the strictest standards and best practices. Microsoft has incorporated significant, complex advancements in areas such as "Active Directory" in both the Windows 2003 version of the server operating system and the 2003 version of Exchange.

The Department has only limited experience with these new technologies. Existing staff lack time to adequately study and learn these new technologies while sustaining support for the Department's enterprise network. Several new business processes and operating procedures as well as new network tools will be required to create a new operational framework within the Department's enterprise network.

This request includes funding for two additional network staff, ongoing training dollars for the entire network team, Microsoft's System Management Services software, and technical consulting services. One position will become the system administrator of the automated management tools and new operational framework for Active Directory environments. Once Active Directory is in place, managing the structure and change management will need substantial coordination, especially between headquarters and the regions. The second position will manage the system architecture, structure, and monitor the secure system configuration. Each of these is necessary to implement and manage the upgrade to this more complex network environment and to sustain the network as technology continues to evolve and improve.

Information Technology Security

The Department leverages technology in order to increase operational efficiencies. Technologies such as wireless communication, database software, expanded use of internet and intranet services for application delivery and communication, and data storage devices with increasing capacity are just a few technologies that continue to be implemented by the Department.

However, with this increased utilization of technology to facilitate productivity, comes increased risk and vulnerability of systems and data. The Department recognizes the importance of protecting critical systems from both internal and external security threats. Whether it is a hacker bent on doing damage, or an employee that does not follow security policy, the end result to the Department will still be catastrophic if sensitive information is altered, destroyed, or released.

A security breach of the Department's critical information technology systems could impact public safety or have legal ramifications. The data stored in the Department's information systems is required to support its mission to provide effective correctional programs. The data includes status of offenders, release dates, levels of required supervision, requirements to notify victims and witnesses upon offender status or location changes, and other court mandates such as geographic information about where sex and/or violent offenders may reside upon release. Numerous security gaps were identified in the Department's information security practices by two independent studies. The funding requested in this package would support maintenance of the security program and would develop a strategy to close these gaps.

The following information technology (IT) security components would be addressed:

- Intrusion detection;
- Network perimeter and access auditing;
- Incident response and notification;
- Data encryption;
- Security awareness training;
- Authentication assurance and evaluation of employees handling sensitive data;
- Assurance of adequate separation of duties; and
- Security policy and procedure development and implementation.

Currently, the Department does not have the resources to safeguard its information assets as required by state policy. A preliminary vulnerability assessment conducted in 2003 by a company (IO Active) recommended that 9.6 positions are needed for the Department to manage the safety and security of the information assets and infrastructure. There was also a Health Insurance Portability and Accountability Act (HIPAA) security feasibility study that came to the same conclusion as the other studies. The Department currently has two positions dedicated to this function and believes that there should be at least nine positions to implement security practices properly.

The following outlines the duties of the seven additional positions:

Information Technology Security Officer
The security officer will lead and manage the security unit and provide direction in the design and implementation of the Departments IT Security Program (policies, standards, and guidelines). They will ensure the Department is able to meet the requirements of the Information Services Board (ISB) IT Security Policy and Standards and interact with other state agencies in all security matters. Reporting IT security related incidents and incorporating security training will make security visible and understandable for senior management to understand current and future IT security threats and IT security policy issues.

Information Technology Security Analyst/Architect
This position will be the technical authority for network security across the state in both the local networks and wide area networks. This position will analyze business needs and design security solutions to meet the Department's business requirements from network and computer systems. The position will build secure usable systems that allow access and protects information from alteration or destruction. This position will also supervise the security team and give daily direction.

Information Technology Security Exchange/Internet
Unauthorized network activity occurs every day in many forms, including Internet abuse. This activity includes using applications that pose a security breech to the network, virus or worm activity that can cause a service outage, and staff exploring the network to see how much they can get to or get away with. This is not internet monitoring because these activities happen within the Department's network. Having a position to watch the network will give the opportunity to recognize and take action for unauthorized network use. The main goal is to provide continued availability and ensure the integrity of Department information.

Security Systems Specialist
Security specialists need software and hardware tools to assist them in effectively and efficiently detecting and recognizing network threats and abuse. The proper installation, maintenance, and administration of these tools make it possible for security analyst and monitors to see security threats and respond to network, systems, and information.

Information Technology Security Policy/Training
The first step to good security is having good security policies. Without policies staff can use and abuse the network without concern for potential corrective action. Imagine an institution without officers, without rules, without order. Policies give management the authority to determine the proper use of information technology and the proper protection of information.

Information Technology Recovery
This position will prepare the Department's hardware and software for a natural or man-made disaster that would wipe out systems or data, by implementing the Department's Business Continuity Plan. The Department will be able to continue managing offenders and their programs by moving the headquarters systems operations to another location.

Information Technology Security Forensics
Events occur with computers and server systems that need detailed investigation into the cause of a security breech or to verify supporting information in a case of abuse. This position will implement the tools and analysis of forensic research on computer systems that have been involved in an information technology security incident. This could lead to corrective actions for employees and to

a deeper understanding of how intruders penetrate computer systems, thus giving us the opportunity to better protect our computer systems.

The Department is required by ISB to have a security audit every three years and findings must be reported to the State Auditor's Office. Agencies that do not maintain an IT Security Program will have their spending authority withdrawn.

Narrative Justification and Impact Statement

How contributes to strategic plan:
This request is critical to agency activities, the strategic plan, and statewide results. The request ensures that the Department has the necessary resources to maintain current levels of service and performance.

This request is required to sustain the agency activities *Confine Convicted Adults in State Prisons, Health Core Services for Adults in State Prisons, Education of Convicted Adults in State Prisons, Supervise High-Risk Adult Offenders in the Community, Supervise Moderate-Risk Adult Offenders in the Community, Supervise Low-Risk Adult Offenders in the Community* and *Corrections-Core Administration*. The resources identified will be directed to support the agency objective to adhere to American Correctional Association standards for facilities and the field to reduce liability so that resources are used/deployed efficiently, effectively, and with regard to meeting constitutional mandates. This objective and strategy moves the Department closer to meeting its high-level organizational goal to enhance organizational capacity and competency. This high-level goal is an intermediate outcome and helps achieve statewide results that improve the safety of people and property.

Performance Measure Detail
No measures were submitted for this package.

Reason for change:
Fire Inspection
The funds requested are necessary to be in compliance with NFPA code 72.

Interstate Compact Requirements
The Interstate Compact Commission adopted new requirements, which increases workload on the Department's Interstate Compact Unit to comply with the new rules.

Exchange Upgrade
The DIS will require the Department to upgrade from Exchange 5.5 to remain on the "Washington State Forest" as Microsoft has discontinued support for Exchange 5.5. The Department desires to maintain its presence in the "Forest" and move off of the unsupported Exchange platform. In order to implement Exchange 2003 across the Department's network, all servers must also be upgraded to the Windows 2003 Server operating system and 12 new servers will be required.

Information Technology Security
The Department is required by ISB policy to maintain an IT Security Program. The program was developed and requires maintenance. Ongoing maintenance of the IT Security Program is currently unfunded. Lack of a good security program will leave the Department vulnerable to security attacks. As a result of being vulnerable, the Department may not be able to perform critical business functions if information systems are disrupted due to a security breach, virus, worm, or other attacks. There may be serious consequences of any internal or external attacks that bring down systems or makes data inaccessible even for a limited number of hours. Disruption of access to systems and data could easily

result in jeopardizing the safety and security of employees and the public, a fiscal impact due to a loss in staff productivity, as well as, a loss of data or information that can not be replaced.

Impact on clients and services:
Interstate Compact Requirements
The Department will be able to effectively administer the increased requirements, and comply with the new rules adopted by the Commission.

Exchange Upgrade
This item would ensure the Department is able to continue services and improve the Department's ability to share information with other agencies in carrying out its mission to protect public safety.

IT Security
Proper security maintenance protects the confidentiality, integrity, and availability of the Department's data by reducing the risk of a breach in security. Availability of data enhances productivity and maintaining the integrity of the data increases the level of confidence in the reliability of the data.

Impact on other state programs:
This change would sustain, even improve, the Department's ability to share information with other state agencies in a secure manner. The ISB security policy requires each agency that shares systems or data to certify that security requirements are being met. Failure to maintain the security policy and conduct security audits will place the Department in risk of not being able to supply data to agencies that request information or use our systems. The state is moving to Active Directory with the goal of being able to easily share data between state agencies. The Department has requested funding in a separate decision packet to become compliant with the requests of Active Directory.

Relationship to capital budget:
N/A

Required changes to existing RCW, WAC, contract, or plan:
N/A

Alternatives explored by agency:
Information Technology Security
The Department has considered outsourcing portions of the security requirements but found these services to be too costly.

Budget impacts in future biennia:
Fire Inspection
Funding will be required in future biennia in order to stay in compliance.

Interstate Compact Requirements
Funding will be required in future biennia in order to manage the increased workload.

Exchange Upgrade
Ongoing costs noted in this request would increase the Department’s carry-forward level budget in future biennia. These costs include the two new positions for network staff, an increased amount of training dollars for the network team, a slight increase in the network equipment replacement budget, and license renewals and support for the new software.

Information Technology Security
All costs will carry forward to future biennia with the exception of the one-time start-up costs. Additional impacts in future biennia may be dependent on the security policy and standards established by the ISB, which may require additional equipment to meet minimum levels of security. Security is a rapidly changing technology and strategy to protect systems and data.

Distinction between one-time and ongoing costs:
Fire Inspection
The costs are ongoing.

Interstate Compact Requirements
The costs are ongoing.

Exchange Upgrade
One time costs comprise the bulk of costs represented in this request. They include the initial expenditures associated with establishing new positions, the initial purchase of Exchange 2003, 12 new servers, and the consulting services necessary to help manage implementation of the upgrade.

On-going costs are necessary to sustain this investment into the future.

Information Technology Security
The start-up costs associated with the seven positions are one-time costs. All other costs associated with the positions and yearly security assessment are assumed to be on-going.

Effects of non-funding:
Fire Inspection
Reductions would be required in other Institutional Services' programs in order to meet regulatory compliance requirements.

Interstate Compact Requirements
Non-funding of this proposal will put Washington State out of compliance with the rules required by the Interstate Compact Commission and as such, will be subject to fines, fees, and costs in such amounts deemed reasonable as fixed by the Interstate Compact Commission.

Exchange Upgrade
If the Department does not upgrade to Exchange 2003, it will be removed from the "Washington State Forest." The impact of this will be felt immediately because the Department will no longer be on the Global Address List. More importantly, removal from the "Forest" would prevent the Department from participating in initiatives such as single sign-on and would preclude the Department from sharing applications through a trusted network that spans all agencies. Having to remain on the unsupported version 5.5 of Exchange would also mean continued exposure to system failure that could affect all email functions in the Department.

If the Department is not able to add 12 new domain controllers, it will not comply with recommended standards, which may prevent the Department from being certified to join the "Washington State Forest." If funding for consulting and two new positions is not received, the integrity of the Department's network may suffer and/or services to customers in other areas of IT, such as desktop users, will degrade.

Information Technology Security:
The data on the Department's IT systems will remain vulnerable to misuse or compromise. A breach in security may compromise the integrity of Department's data and could have legal ramifications. A

serious breach in security may cause the Department's IT systems to become inoperable preventing the Department from performing many of its IT dependent business functions. Information concerning offenders may be corrupted or may not be available which could adversely affect public safety. Below are several possible scenarios:

- Criminal justice agencies may be given inaccurate data or not be able to obtain offender data.
- Community corrections officers (CCOs) may not know about mandates required by the courts.
- Public safety could be affected if offenders are not supervised at the appropriate level.
- The Department may not be able to provide accurate information on the location and the release of violent and/or sex offenders.

Expenditure Calculations and Assumptions:

Fire Inspection

The Department anticipates the cost associated with this change to be $34,000 for the biennium to perform the testing required.

Interstate Compact Requirements

Based on the current workload of 3,145 cases per year the Department has to process, it is assumed that each case will take an additional average of 1.36 hours to process, for a total of 4,277 staff hours per year. The result is the request for an additional 3.0 FTEs.

Exchange Upgrade

This proposal is based on the following assumptions:

1. The staffing costs include funding for two positions (Information Technology Systems Specialist 6 and Information Technology Systems Specialist 5), including salaries, benefits, goods and services, and travel. These positions will function as the Advanced System Architect of Active Directory. The second position will function as the advanced System Administrator of the automated management tools and new operational framework for Active Directory.
2. Funding is requested for software, software tools, and training to provide the agency internal expertise to aide in troubleshooting.

Information Technology Security

1. The staffing costs include funding for seven positions.
2. Funding is also requested to have a security assessment completed every other year by an independent auditor to ensure the Department is compliant with ISB standards at an estimated cost of $50,000.

Object Detail	**FY 2006**	**FY 2007**	**Total**
A Salaries and Wages	$627,000	$627,000	$1,254,000
B Employee Benefits	$182,000	$182,000	$364,000
C Personal Service Contracts	$440,000	$50,000	$490,000
E Goods and Services	$504,000	$188,000	$692,000
G Travel	$12,000	$12,000	$24,000
J Capital Outlays	$594,000	$65,000	$659,000
Total Objects	**$2,359,000**	**$1,124,000**	**$3,483,000**